UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
and Does 1-15,

Defendants.

Civil Action No.

REDACTED

DECLARATION OF SHANE HUNTLEY

I, Shane Huntley, declare as follows:

1. I am the Director and Lead of Google's Threat Analysis Group ("TAG"). I submit this declaration in support of Google's Application for an Emergency Temporary Restraining Order and Order To Show Cause for a Preliminary Injunction. I have personal knowledge of the matters discussed in this declaration, and if called as a witness, I could and would testify competently to the matters discussed in this declaration.

2. As the Director and Lead of TAG, I evaluate cybersecurity threats to Google products and services, including Google Search, Gmail, YouTube, Chrome, Google Ads, Google Drive, and Google Maps, as well as the risks to Google and its billions of users posed by those threats. I am responsible for protecting Google users, products, services, platforms, and assets from serious cyberattacks, including botnet attacks. I have worked at Google for over 11 years, starting as a Security Software Engineer for TAG in 2010, and worked in that group until I became Director in November 2017. I have been in my current position for four years. While at Google, I have participated in and directed botnet investigations and disruptions.

3. Before joining Google, I worked for over five years as a security software engineer for the Australian Government, and for two years as a computer security research scientist for the Defense Science and Technology Organization. I obtained a bachelor's degree in engineering from the University of New South Wales.

4. Under my direction, TAG has investigated the structure and function of a botnet called "Glupteba." TAG has assessed the activities of this botnet and the

impact it has on Google and Google users. Our investigation has determined that the Glupteba botnet currently involves approximately one million compromised devices worldwide. We estimate that, in September 2021, the botnet was growing at a rate of thousands of new infections per day. We also estimate that the botnet has led to thousands of compromised Google and social media accounts. We have concluded that the Glupteba botnet has caused significant damage to Google and other parties, and that it is a powerful vector for more serious harm if it is permitted to operate unimpeded.

I. Google Products and Background

5. Google is recognized as a worldwide leader in technology. Cutting-edge innovation and development drove the company's growth. We maintain our position at the forefront of multiple sectors through a sustained commitment to offering products that are both dependable and advanced. Google has pioneered technologies used by millions of people including Android, Chrome, Gmail, Google Drive, Google Maps, Google Photos, Google Play, Search, and YouTube:

a. **Android**: Android is an operating system that is designed to run on mobile devices, such as smartphones or tablets. Android generates revenue in part through advertising on the platform.

b. **Chrome**: Chrome is a web browser that runs on various operating systems, including on personal computers, smartphones, and tablets.

c. **Google Cloud**: Google Cloud is a suite of cloud services including computing, data storage and analytics, and machine learning.

d. **Gmail**: Gmail is an email service that is hosted on Google's servers.

e. **Google Drive**: Google Drive is a file storage service that allows users to host and share files in various formats on Google's servers. These files can be created, accessed, and edited remotely.

f. **Google Search**: Google Search is an internet-based search engine that allows users to search for publicly accessible documents and websites indexed by Google's servers.

g. **Google Workspace**: Google Workspace is a cloud-based suite of productivity and collaboration tools for businesses. This service provides businesses with custom email accounts with integrated collaboration tools, including Gmail, Google Calendar, Google Meet, Google Chat, Google Drive, Google Docs, Google Sheets, Google Slides, Google Forms, and Google Sites.

h. **YouTube**: YouTube is an online video sharing platform.

i. **Google Ads**: Google Ads is an online advertising platform through which advertisers can publish advertisements on various Google platforms including, for example, Google Search and YouTube.

II. Google's Commitment to Cybersecurity

6. For the past two decades, Google has made security the cornerstone of our business. Our commitment to security begins with our product strategy. The company does not simply respond to security incidents or plug security holes. Instead, Google works to eliminate entire classes of threats for users and businesses

whose work depends on our services. We strive to keep our users safe by making our products secure by default—by using progressive layers of both digital and physical protection to block malware, phishing attempts, spam messages, and cyberattacks, and by employing the best engineers in the world.

7. Google dedicates significant resources to privacy and security incident response to mitigate cyberattacks. We also invest substantial resources in safety, security, and content review efforts to combat misuse of Google's services and unauthorized access to user data by third parties. These efforts include investigations and reviews of platform applications that could access the information of users of our services.

8. Google also has dedicated resources to thwarting attacks that result from the operation of botnets. For example, Google's "Project Shield" is a free service that protects websites from distributed denial of service ("DDoS") attacks, which often are perpetrated by botnets.[1] Similarly, Google Cloud Armor Adaptive Protection helps protect Google Cloud applications, websites, and services against DDoS attacks such as HTTP floods and other high-frequency application-level malicious activity.[2]

9. Because the cyber threat landscape is constantly evolving, Google has also devoted significant resources to detecting potential cybersecurity threats, rapidly

[1] Charlie Osborne, *Google Pulls Krebs on Security Out of the Abyss*, ZDNet (Sept. 25, 2016), https://www.zdnet.com/article/google-rescues-krebs-on-security-from-the-abyss.

[2] *Google Cloud Armor Adaptive Protection Overview*, Google Cloud, https://cloud.google.com/armor/docs/adaptive-protection-overview (last visited Nov. 16, 2021).

countering them, and informing the broader information security community about them. We have published over 160 academic research papers on computer security, privacy, and abuse prevention, and we warn other software companies of weaknesses in their systems.

10. TAG is central to that effort. TAG tracks more than 270 targeted or government-backed attacker groups from more than fifty countries and hundreds of financially motivated actors. It is among the world's most sophisticated cyber threat analysis teams, and combines threat intelligence, malware analysis, and engineering of large-scale malware and threat-analysis systems to defend our services, infrastructure, and users from advanced disinformation campaigns, hacking, financially motivated abuse, and other cyber threats.

11. TAG also analyzes hacking techniques and other clues to the groups' identities to thwart attacks. To track and investigate cybersecurity threats, TAG leverages data across widely used Google products, including VirusTotal, a database of malicious code. As part of its efforts, TAG regularly works with law enforcement agencies, national security entities, and private-sector cybersecurity partners across the world.

12. These investigations have succeeded in neutralizing major cybersecurity threats, including foreign nation-state disinformation and threat actors who targeted or impersonated health organizations during the COVID-19 pandemic. For example, in early 2021, TAG disrupted efforts by APT35, an advanced persistent threat actor backed by Iran and known to have targeted campaign staffers during the United

States' 2020 elections.[3] TAG also has a proven track record in identifying and disrupting campaigns utilizing previously unidentified zero-day exploits, such as when it identified and disrupted an attack against targets in Armenia.[4] TAG sends Google users warnings when they are targeted by nation-state actors; so far in 2021, TAG has sent over 50,000 warnings to users, a nearly 33% increase from this time in 2020.

III. The Glupteba Botnet

13. A botnet is a network of devices connected to the internet that have been infected with a type of malicious software (or "malware") that places them under the control of persons who can then use the infected devices for malicious purposes, such as to commit fraud or engage in disinformation campaigns. The "bot controllers" who operate the botnet typically do so through a "command and control" server (the "C2 server"). The C2 server sends instructions to the bots on the infected devices, which in turn carry out those instructions.

14. Some of the largest botnets have conscripted millions of devices, often unbeknownst to their owners. As a result, a botnet can marshal an astonishing amount of computing power in service of a wide variety of illegal activities, including attacking other devices, installing other forms of malicious software, performing DDoS attacks, stealing credentials or financial information, selling or renting access

[3] Ajax Bash, *Countering Threats from Iran*, Google (Oct. 14, 2021), https://blog.google/threat-analysis-group/countering-threats-iran/.

[4] Maddie Stone & Clement Lecigne, *How We Protect Users from 0-Day Attacks*, Google (July 14, 2021), https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

to the infected devices to other cybercriminals, mining cryptocurrency, sending spam, and distributing ransomware.

15. One malware family—called "Glupteba"—has several different variants that cybersecurity researchers have observed for at least a decade.

16. In recent years, and beginning no later than 2019, cybercriminals (referred to herein as the "Glupteba Enterprise" or the "Enterprise") have weaponized the Glupteba malware to support a massive and sophisticated botnet (the "Glupteba botnet") that can be tailored to serve numerous criminal purposes, including user credential or data theft and hijacking devices to mine cryptocurrency.

17. The Glupteba botnet uses numerous domains to disseminate malware, most of which are registered with different registrars using a variety of Gmail accounts. Once infected with the malware, a device becomes part of the Glupteba botnet.

18. I estimate that TAG has spent more than 2,000 engineering hours combatting the Glupteba botnet to protect Google users and others. This does not include the other security teams at Google who also have worked to combat the Glupteba Enterprise's harms against our users.

19. TAG took several steps to investigate and contain the Glupteba botnet. As part of Google's investigation into the Glupteba botnet, for instance, TAG analyzed numerous samples of Glupteba malware, and reverse-engineered and examined its

code in order to identify hard-coded domains.[5] Our investigation also involved intentionally infecting devices in order to understand how infected machines are affected, damaged, and controlled by the Glupteba botnet. Using that analysis, we monitored each infected device's internet traffic and activity to determine how it downloads other malware components, how it communicates with other Glupteba-infected devices, and with which other devices it communicates. In other words, we sought to understand how a device in the botnet is used by the botnet and controlled by the Enterprise. To protect Google users and infrastructure, we took steps to detect and track malicious activity over time.

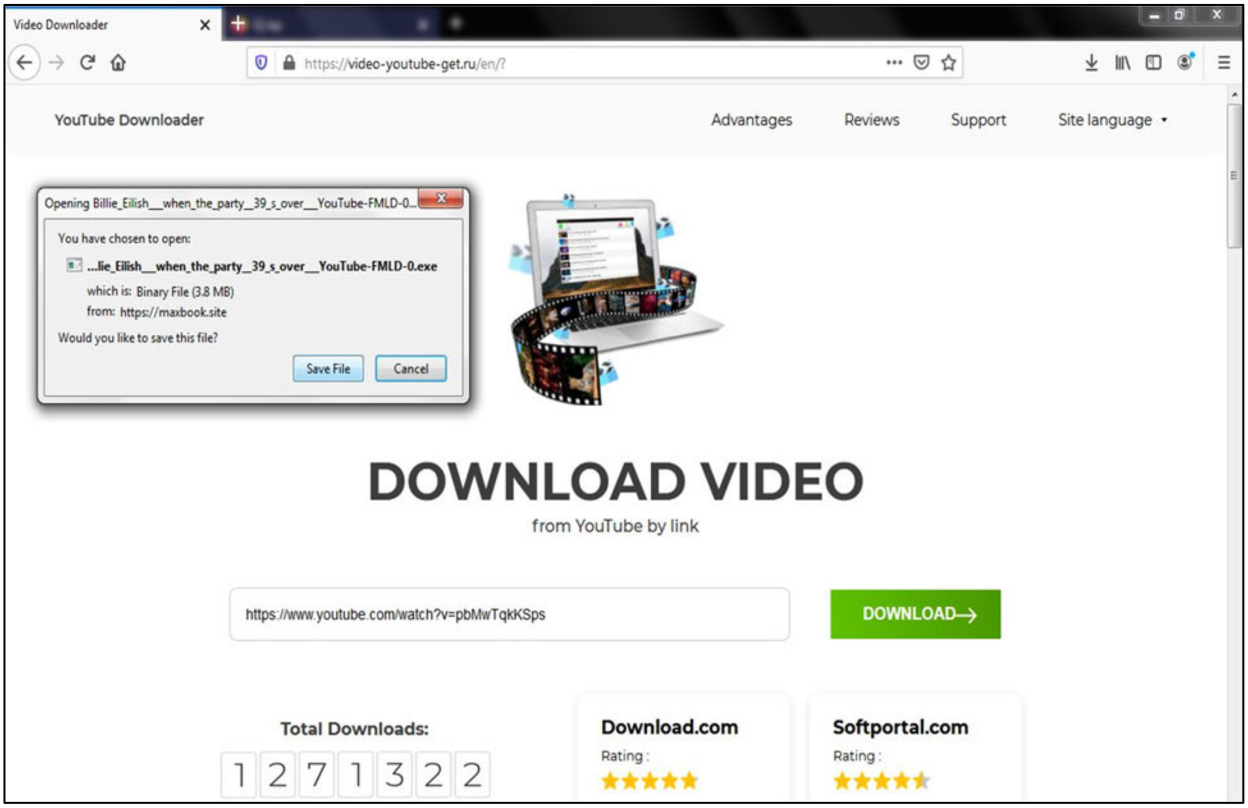
20. My conclusions concerning the Glupteba botnet's activity and capabilities are based on TAG's investigation and observations.

21. Google observed the delivery of Glupteba malware in the summer of 2020 on numerous sites for downloading software or videos or streaming movies. Those sites often advertised "free downloads" for the purpose of infecting devices and recruiting them to the Glupteba botnet.

22. Glupteba malware conceals itself as free downloadable software that tricks users into inadvertently infecting their device with the malware. For example, users that attempt to download a free game will unknowingly be redirected to servers hosting Glupteba malware code, resulting in the download and installation of the malware.

[5] TAG's investigation included analysis of the Glupteba binary file, which is the executable program code that contains instructions for the malware to run in a device.

23. The Glupteba Enterprise has leveraged Google's well-known marks to facilitate malware distribution. For instance, at the website located at "video-youtube-get.ru," users are deceived into believing they are downloading a YouTube video, and instead, the user unknowingly downloads and installs Glupteba malware. Below is a true and correct image of an excerpt from the website, with a screenshot of a Glupteba malware download masquerading as a YouTube video:



Opening Billie_Eilish__when_the_party__39_s_over__YouTube-FMLD-0...

You have chosen to open:

...lie_Eilish__when_the_party__39_s_over__YouTube-FMLD-0.exe

which is: Binary File (3.8 MB)
from: https://maxbook.site

Would you like to save this file?

https://www.youtube.com/watch?v=pbMwTqkKSps

24. When the unsuspecting victim clicks on the link, the malware is delivered via "droppers." Droppers are an electronic Trojan horse. They appear as legitimate applications to the user, but once downloaded, they deliver malware to the user's device.

25. Once installed on a device, Glupteba malware evades being detected by the device's owner and its antivirus software. It manipulates the device's operating system by hiding the malware's existence and preventing it from showing up on an infected device's security logs. It can avoid cybersecurity detection tools, anti-virus software, and system monitoring programs, including security software featured in popular operating systems. Glupteba malware not only evades detection once it is installed, but it also spreads to other devices on the same network as the infected device.

26. The Glupteba malware that is installed on infected devices is software consisting of computer coding. Contained within that coding, or "hard-coded" in the malware, are various domain names[6] that direct the botnet to servers—C2 servers and content delivery network ("CDN") servers—that provide instructions and updates to the botnet. The domain names that are hard-coded in the malware can be refreshed through backdoor functions[7] or querying the blockchain, explained *infra* at paragraphs 33 to 42.

27. Through our investigation, Google identified numerous domains and IP addresses used as part of_this infrastructure. The known domains and IP addresses are listed in **Appendix A**.[8] The IP addresses where some of the Glupteba

[6] The domain name is a "pointer" to an IP address where a server is hosted.

[7] Backdoor functions are covert methods of bypassing normal authentication or encryption in an internet-connected device.

[8] Appendix A includes domains used for C2 and CDN server communication and operation, as well as domains used for distribution of the Glupteba malware and domains used for the Enterprise's criminal schemes.

infrastructure is hosted belong to a German web hosting provider. Google also has identified relevant "nameservers," which are server components that translate domain names into IP addresses. The relevant nameservers belong to a U.S. web infrastructure company.

28. Once installed, Glupteba malware utilizes numerous modules (which are downloaded through the CDN servers) to undertake its activities.

29. In the course of its investigation, TAG performed manual malware analysis on 36 different modules. The modules are compiled programs that use multiple programming languages including Go and C++. During its investigation, TAG performed manual malware analysis on 36 different modules.

30. The program responsible for installing the Glupteba malware modules uses various mechanisms to avoid being detected by security products or automated analysis tools. TAG calls this program the main dropper. This dropper can check for the presence of installed antivirus programs, add firewall rules to let its communication through, and shut down Microsoft's native security program, Windows Defender. The main dropper also has capabilities to detect tools often used by malware analysts, including Sysinternal tools, a suite of free administrative programs offered by Microsoft.

31. My team is aware of the following types of modules that are installed as part of the Glupteba malware and botnet:

a. Modules that scan for certain known vulnerabilities on the local network's hardware and software and then exploit those vulnerabilities using variants of EternalBlue (a computer virus) to distribute itself across the local network.

b. Modules that attempt to gain access to the local network by trying to log in to the secure shell ("SSH").

c. Modules that steal Google Chrome browser data, including cookies, credentials and passwords, and attempt to install a Google Chrome browser extension.

   i. The module responsible for stealing Chrome data is written in Go. It reads the user data from an infected system's drive and uploads it to a C2 server using the HTTP protocol.

d. Modules that deploy proxies onto the infected machine so that it can be remotely directed by the bot controllers.

   i. The proxy deployment module is written using the C++ programming language. The proxy program registers to its server using the HTTP protocol and can afterward be used to proxy traffic coming from the established tunnel.

   ii. Another proxy module written in Go deploys a peer-to-peer connection for proxying.

e. Modules that scan a device's network to exploit routers (*e.g.*, MicroTik routers) so that they can be used to proxy malicious traffic without the router owner's knowledge.

f. Modules that mine cryptocurrency using the infected device's processing power and electricity source.

32. Once the modules are downloaded to the infected device via the CDN server, the C2 server then commands the infected device to use the modules. For example, the C2 server could activate the module that steals the device's account credentials or the module that mines Bitcoin, depending on the Glupteba Enterprise's plans for the infected device.

IV. The Glupteba Botnet Exploits Blockchain Technology

33. TAG's analysis of Glupteba malware indicates that the Glupteba botnet uses blockchain to protect the bot controller's ability to issue commands to the infected devices.

34. In the classic botnet structure, the botnet can no longer function when the bot controller's C2 server is shut down because the C2 server cannot communicate instructions to the botnet. To avoid this predicament and protect their botnets, bot controllers have developed numerous techniques to protect or quickly change their C2 servers. A common method is to simultaneously use many domains as C2 servers, such that the disruption of a single C2 server will not disrupt the botnet's operations.

35. The Glupteba botnet innovates beyond these techniques and uses a method incorporating blockchain technology. The Glupteba botnet's use of blockchain makes it particularly difficult to disrupt by reducing its reliance on pre-determined domains.

36. Blockchains are decentralized databases spread over a network of participants that are often used to record cryptocurrency transactions. A person seeking to transact using cryptocurrency will do so on the blockchain through a digital “wallet”; that transaction will be recorded in the blockchain, leaving a public record. Wallets store the public and private “keys” used to send and receive cryptocurrency. A public key, or “address,” is akin to a bank account number, and a private key is akin to a PIN or password that allows a user to access and transfer value associated with the public address.

37. The Glupteba botnet uses the blockchain to protect itself against disruption through coding in the Glupteba malware that instructs infected devices to look to specific addresses in wallets on the blockchain to identify the next C2 server when the botnet is not able to communicate with the original (or last-functioning) C2 server.

38. When an infected device is unable to communicate with the C2 server, Glupteba malware instructs the device to query the public blockchain for three Bitcoin addresses:

a. 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6

b. 1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1

c. 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97

39. These Bitcoin addresses are controlled by the cybercriminals behind the Glupteba botnet. The malware queries these addresses using the publicly accessible blockchain.

40. The cybercriminals behind the Glupteba botnet periodically make small Bitcoin transactions from these addresses. When they do so, they input an encrypted code in a field in the Bitcoin blockchain typically used for notes or messages, akin to the "memo" line of a check, or the payment note in a digital payment application like Google Pay (*e.g.*, "for groceries"). When decrypted, this code contains the address of a back-up C2 server. The information is either sent as a standalone, valueless data transmission, or it accompanies a transaction in which funds are exchanged.

41. The 256-bit AES decryption key is embedded in the Glupteba malware, so the infected devices that comprise the Glupteba botnet can read the encrypted messages associated with the Bitcoin transactions and identify the back-up C2 server.

42. Accordingly, if a C2 server is taken offline, the Glupteba botnet can locate a replacement C2 server by querying the public blockchain, identifying transactions that involve Bitcoin addresses operated by the bot controllers, and then decrypting the identity of the next C2 server.

V. Criminal Schemes Perpetrated by the Glupteba Botnet

43. TAG's investigation into the Glupteba botnet revealed various criminal schemes carried out by the Glupteba Enterprise, which consists of several individuals and corporations. The Enterprise operates and uses the botnet to carry out criminal schemes and to further the criminal schemes of others.

44. As described below, the Enterprise uses the botnet to effect at least five criminal schemes: (1) the Stolen Accounts Scheme, (2) the Credit Card Fraud Scheme,

(3) the Disruptive Ad Scheme, (4) the Proxy Scheme, and (5) the Cryptojacking Scheme.

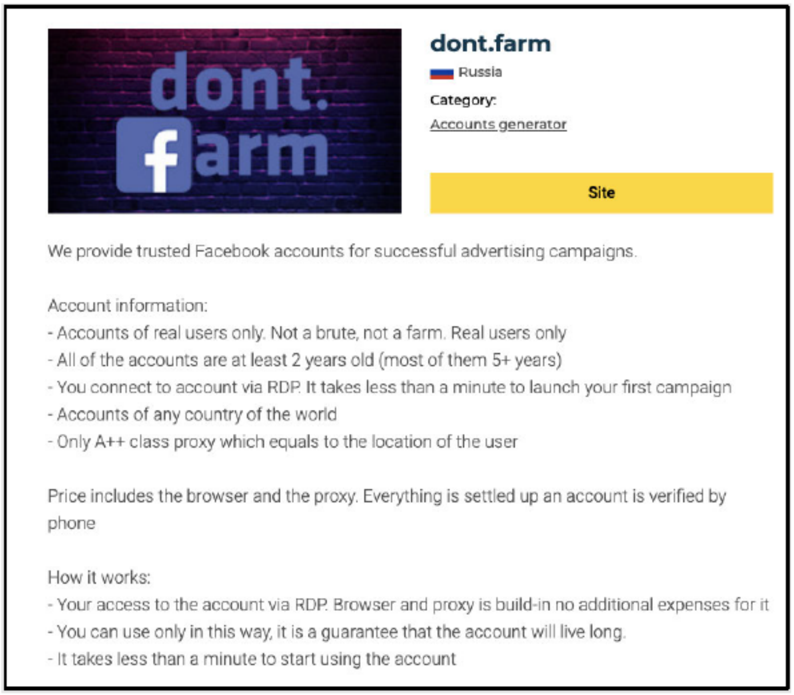
Stolen Accounts Scheme

45. The Glupteba malware steals login credentials and login cookies for a range of accounts, including Google and other accounts, from infected devices. With this information, the Glupteba Enterprise has the capacity to log in to the user's account as though it is the user. The Enterprise loads these hijacked accounts onto open browsers operating on virtual machines. A virtual machine is similar to a physical computer; however, the operating system of the virtual machine is contained within another computing environment, typically on a cloud computing platform. Like typical computers, the Enterprise's virtual machines have a web browser. In the open browser, the Glupteba Enterprise enters the username and password for a Google account (or other account) that Glupteba malware has stolen. The Enterprise then sells access to the stolen account through a website that it operates, Dont.farm, thereby enabling cybercriminals and other customers the ability to exploit the stolen account.[9] Once granted access to the virtual machine, the Dont.farm customer has free rein to use the hijacked account as desired, including to launch fraudulent ad campaigns.

46. Dont.farm confesses publicly that it is selling access to other people's accounts, as the website is a storefront for the sale of such access. Below are true and

[9] See Exhibit 1, which is a true and correct copy of the webpage Dont.farm as of November 3, 2021.

correct copies of excerpts from Dont.farm's public advertising[10] and from the Dont.farm website, respectively:



dont.farm

Russia

Category:

Accounts generator

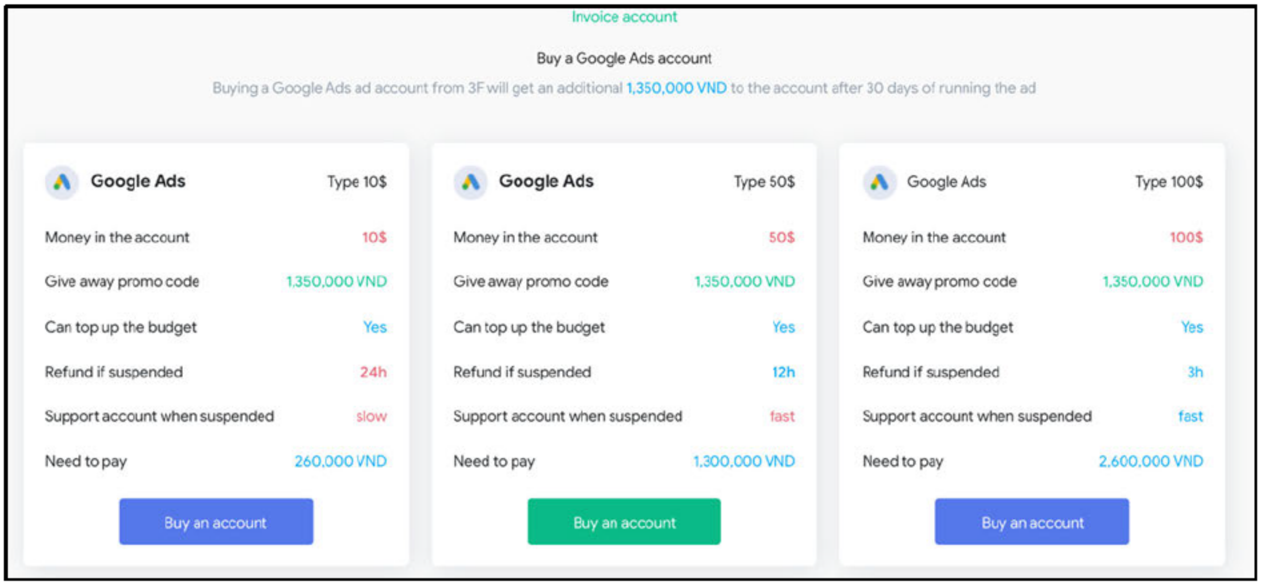
Site

We provide trusted Facebook accounts for successful advertising campaigns.

Account information:
- Accounts of real users only. Not a brute, not a farm. Real users only
- All of the accounts are at least 2 years old (most of them 5+ years)
- You connect to account via RDP. It takes less than a minute to launch your first campaign
- Accounts of any country of the world
- Only A++ class proxy which equals to the location of the user

Price includes the browser and the proxy. Everything is settled up an account is verified by phone

How it works:
- Your access to the account via RDP. Browser and proxy is build-in no additional expenses for it
- You can use only in this way, it is a guarantee that the account will live long.
- It takes less than a minute to start using the account



Invoice account

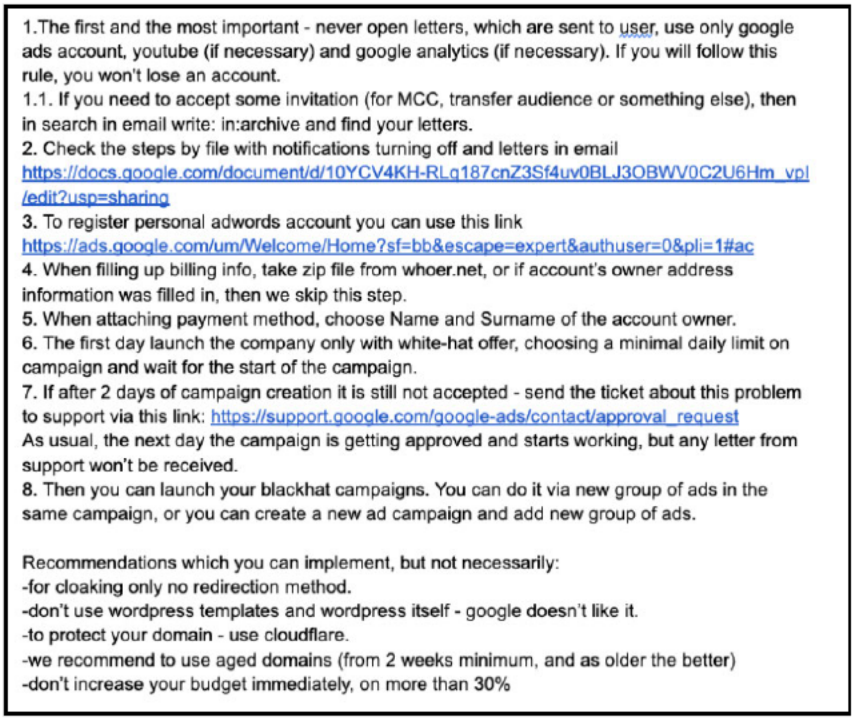
Buy a Google Ads account

Buying a Google Ads ad account from 3F will get an additional 1,350,000 VND to the account after 30 days of running the ad

Google Ads	Type 10$	Google Ads	Type 50$	Google Ads	Type 100$
Money in the account	10$	Money in the account	50$	Money in the account	100$
Give away promo code	1,350,000 VND	Give away promo code	1,350,000 VND	Give away promo code	1,350,000 VND
Can top up the budget	Yes	Can top up the budget	Yes	Can top up the budget	Yes
Refund if suspended	24h	Refund if suspended	12h	Refund if suspended	3h
Support account when suspended	slow	Support account when suspended	fast	Support account when suspended	fast
Need to pay	260,000 VND	Need to pay	1,300,000 VND	Need to pay	2,600,000 VND
Buy an account		Buy an account		Buy an account	

[10] See Exhibit 2, which is a true and correct copy of the webpage https://affbank.com/affiliate-services/dontfarm as of November 24, 2021.

47. The Dont.farm website also provides a manual for how to exploit accounts while minimizing the risk of getting discovered by the owner or the service provider. Below is a true and correct copy of an excerpt from the Dont.farm website[11]:

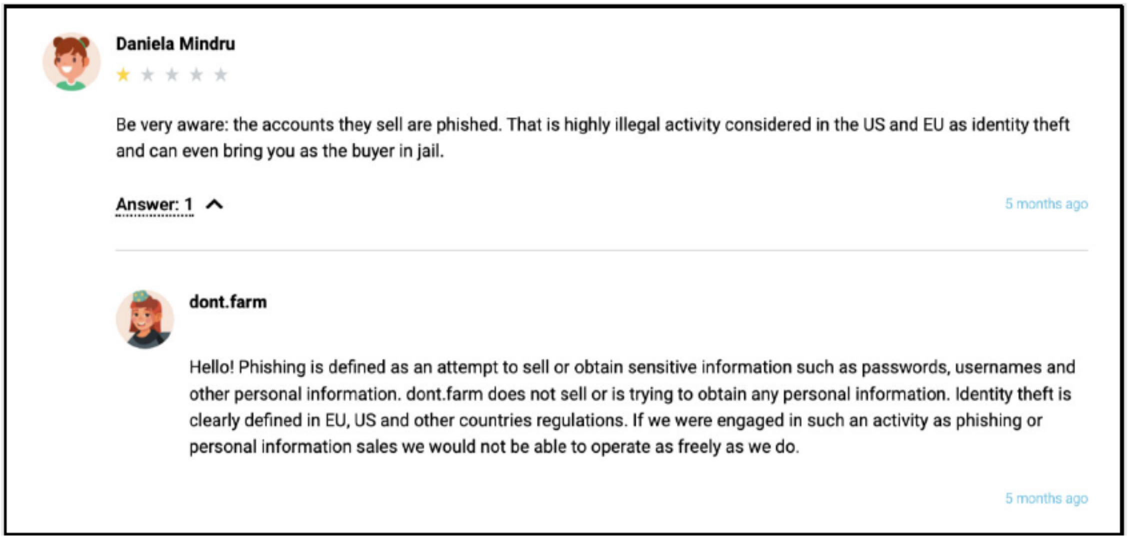


1.The first and the most important - never open letters, which are sent to user, use only google ads account, youtube (if necessary) and google analytics (if necessary). If you will follow this rule, you won't lose an account.
1.1. If you need to accept some invitation (for MCC, transfer audience or something else), then in search in email write: in:archive and find your letters.
2. Check the steps by file with notifications turning off and letters in email https://docs.google.com/document/d/10YCV4KH-RLq187cnZ3Sf4uv0BLJ3OBWV0C2U6Hm_vpl/edit?usp=sharing
3. To register personal adwords account you can use this link https://ads.google.com/um/Welcome/Home?sf=bb&escape=expert&authuser=0&pli=1#ac
4. When filling up billing info, take zip file from whoer.net, or if account's owner address information was filled in, then we skip this step.
5. When attaching payment method, choose Name and Surname of the account owner.
6. The first day launch the company only with white-hat offer, choosing a minimal daily limit on campaign and wait for the start of the campaign.
7. If after 2 days of campaign creation it is still not accepted - send the ticket about this problem to support via this link: https://support.google.com/google-ads/contact/approval_request
As usual, the next day the campaign is getting approved and starts working, but any letter from support won't be received.
8. Then you can launch your blackhat campaigns. You can do it via new group of ads in the same campaign, or you can create a new ad campaign and add new group of ads.

Recommendations which you can implement, but not necessarily:
-for cloaking only no redirection method.
-don't use wordpress templates and wordpress itself - google doesn't like it.
-to protect your domain - use cloudflare.
-we recommend to use aged domains (from 2 weeks minimum, and as older the better)
-don't increase your budget immediately, on more than 30%

48. In response to a public comment accusing Dont.farm of illegal activity, Dont.farm attempted to defend its criminal conduct as legitimate[12]:

[11] See Exhibit 3, which is a true and correct copy of a manual provided by Dont.farm to customers using stolen Google accounts.
[12] *See* Exhibit 2.



Daniela Mindru

★★★★★

Be very aware: the accounts they sell are phished. That is highly illegal activity considered in the US and EU as identity theft and can even bring you as the buyer in jail.

Answer: 1 5 months ago

dont.farm

Hello! Phishing is defined as an attempt to sell or obtain sensitive information such as passwords, usernames and other personal information. dont.farm does not sell or is trying to obtain any personal information. Identity theft is clearly defined in EU, US and other countries regulations. If we were engaged in such an activity as phishing or personal information sales we would not be able to operate as freely as we do.

5 months ago

49. When customers purchase Dont.farm access, they are instructed to take steps to hide their intrusion. For example, they are instructed to archive emails from "google.com" and "ads-reply@google.com" so that any alert emails from Google to the true user of the account will not be noticed. Furthermore, the Dont.farm customer is instructed to turn off account notifications for Google Ads and YouTube services, again, so that the true user of the account will not be notified of any changes made to their account.

50. Dont.farm also provides other directions to their customers to help them avoid detection by Google. For example, they advise not to increase advertising budgets by more than 30 percent, and that any domains used for advertisements should be at least two weeks old, if not significantly older. These statements suggest the operators of Dont.farm believe these steps will help Dont.farm users avoid detection from Google security teams like TAG.

51. TAG estimates that since its creation in 2019, Dont.farm has sold access to hundreds of thousands of stolen accounts for Google and other services.[13] Dont.farm states that it has been in operation since 2019 and has over 200 employees.[14] Dont.farm advertises that customers can use it to obtain access to "accounts of any country in the world."[15]

52. Customers of Dont.farm who pay for access to a stolen account obtain not only access to the stolen account, but also a veil of secrecy provided by a proxy. Specifically, their activity appears to third parties (such as Google) as though it is emanating from the location of the virtual machine, or potentially from the location of a different infected device that is being used in connection with the Proxy Scheme, discussed below. The true location of the customer of Dont.farm is hidden.

53. Dont.farm provides criminals with the opportunity to engage in commercialized ad fraud. They often use this form of ad fraud to phish credentials, such as financial information or other personal information, from buyers. These stolen accounts are potential platforms for many other fraudulent schemes as well.

54. Collectively, it is clear to both the operators of Dont.farm, as well as the users of Dont.farm, that the use of the provided Google and other accounts is illegitimate, and that Dont.farm is a service designed to perpetrate fraud.

[13] See Exhibit 4, which is a true and correct copy of the webpage https://dont.farm/technical as of November 22, 2021.
[14] *See* Exhibit 1.
[15] *See* Exhibit 2.

55. With regard to the Stolen Accounts Scheme, Google specifically found the following through its investigation:

a. Google identified [redacted]@gmail.com as an account being sold by Dont.farm. This Gmail account was created in 2016. It did not initiate use of Google Ads until five years later, on April 21, 2021. On that same day, the account was logged into after four failed password attempts from an IP address in Germany, a location atypical of prior account logins. The very next day, on April 22, 2021, the account had logins from IP addresses tied to the United States and Iran. Review of these logins showed they occurred from a variety of device and browser types. In addition, a review of the Gmail settings on the account indicated it had established a filter to send all emails from google[.]com to trash, consistent with the aforementioned instructions from Dont.farm.

b. Google identified [redacted]@gmail.com as an account being sold by Dont.farm. This Gmail account was created in 2018. It did not initiate use of Google Ads until three years later, on March 30, 2021. On that same day, the account was logged into from a new device. Google's review determined that the Gmail settings on the account indicated it had established filters to send all emails from ads-account-noreply@google[.]com and from google[.]com to trash. Additionally, Google observed a series of failed login attempts for this account in early July 2021 from IP addresses associated with numerous countries, such as Vietnam, Italy, Brazil, Ecuador, Iraq, Czechia, Bangladesh, and the United States.

c. Google identified [redacted]@gmail.com as an account being sold by Dont.farm. This Gmail account was created in 2019. It did not initiate use of Google Ads until two years later, on March 24, 2021. On that same day, the account was logged into from a Windows device in the United Kingdom, a device and location atypical of other logins, including another login that occurred that same day. Gmail settings on the account indicated it had established filters to send all emails from ads-account-noreply@google[.]com and google[.]com to trash.

Credit Card Fraud Scheme

56. The Enterprise operates Extracard.net, a payment fraud service that enables cybercriminals and others to purchase ads from Google Ads that are provided, but not paid for.[16]

57. Extracard.net provides access to credit card numbers that are emitted from a Russian bank. Malicious actors use these credit card numbers to make purchases without paying and to mask their identities. "Clients" of Extracard.net only pay a fraction of the credit card bill.

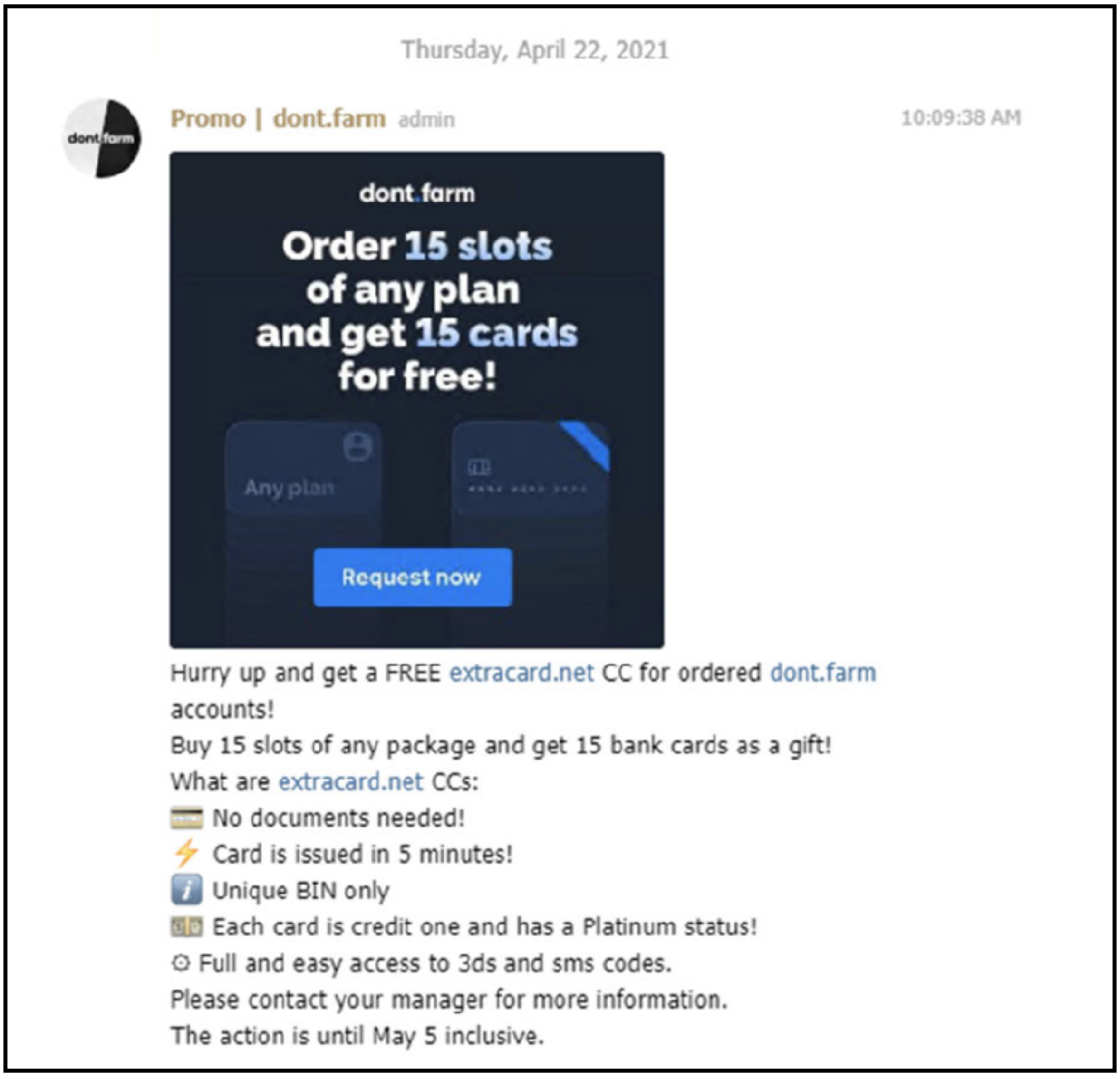
58. A review of Google Ads accounts identified hundreds of Google Ads customers who abused Google's Ad platform through the use of Extracard.net credit

[16] See Exhibit 5, which is a true and correct copy of the webpage https://extracard.net as of November 2, 2021.

cards. A review of the ad campaigns operated by these customers indicated they were often serving malicious or fraudulent ads and thereby harming other Google users.

59. Google provides Google Ads account holders with an advance credit for ad campaigns when an account holder places a credit card on file with the account. The account holder can spend up to the credit amount (within 30 days) before Google charges the credit card on file. When account holders place legitimate credit cards on file, Google can collect the charges when it runs the credit card. When Google seeks to charge credit cards issued by Extracard.net, in contrast, the full charged amount is not paid. By taking advantage of the advance credit system, customers of Google Ads with Extracard.net credit cards on file have been able to "purchase" ad campaigns and execute those ad campaigns without paying, causing monetary loss to Google.

60. The Enterprise uses the Credit Card Fraud Scheme and the Stolen Accounts Scheme in tandem, marketing Extracard.net-issued credit cards to customers of Dont.farm. Below is a true and correct copy of an online advertisement, dated April 22, 2021, marketing Extrcard.net credit cards to users of Dont.farm:



Thursday, April 22, 2021

Promo | dont.farm admin 10:09:38 AM

Hurry up and get a FREE extracard.net CC for ordered dont.farm accounts!
Buy 15 slots of any package and get 15 bank cards as a gift!
What are extracard.net CCs:
💳 No documents needed!
⚡ Card is issued in 5 minutes!
ℹ️ Unique BIN only
💵 Each card is credit one and has a Platinum status!
⚙ Full and easy access to 3ds and sms codes.
Please contact your manager for more information.
The action is until May 5 inclusive.

61. With regard to the Credit Card Fraud Scheme, Google specifically found the following through its investigation:

a. Two Google Ads accounts associated with [redacted]@gmail.com purchased ads using a credit card consistent with credit cards from Extracard.net. Both Ads accounts were suspended for ad cloaking, a technique used to defraud online advertisers and dupe internet users to view malicious sites, often with the purpose of compromising their devices. Upon review, the Ads accounts were found to be running ads which redirected to a cryptocurrency investment scam. Moreover, a review of [redacted]@gmail.com indicated it had logins from IP addresses associated with AWMProxy.net.

b. The Google Ads account associated with [redacted]@gmail.com signed up for Google AdWords using a credit card consistent with credit cards from Extracard.net. The Ads account was suspended for payment fraud because it ran ads worth $410.89 Australian Dollars in mid-September 2021, for which Google never received payment. This account was created just two weeks before it began using Google AdWords and it used VPN IP addresses for logging in, suggesting that the user purposefully masked its identity and likely created the account in order to undertake fraudulent ad activity using the Extracard.net credit card.

c. The Google Ads account associated with [redacted]@gmail.com signed up for Google AdWords using a credit card consistent with credit cards from Extracard.net. The account was suspended for payment fraud because it ran ads worth approximately 2800 EUR between June 4, 2021 and June 18, 2021, for which Google was only partially paid.

Disruptive Ads Scheme

62. The Glupteba Enterprise uses Push.farm, and it previously used Trafspin.com, to place disruptive ads on infected mobile devices.[17] The disruptive ads pop up on the infected device, interrupting and interfering with the user's normal use of that device.

63. When a mobile device is infected with the malware, the Enterprise is able to push web and in-app advertisements to the infected device. This allows the Enterprise to profit by selling advertising space to advertisers, and then by pushing those advertisements to the infected devices.

64. Trafspin.com does not appear to be live. However, there is evidence that the Enterprise is shifting to use a new site, Push.farm, to sell the placement of disruptive ads on mobile devices.

Proxy Scheme

65. The Glupteba Enterprise uses AWMProxy.net[18], and formerly used Abm.net, to rent out IP addresses belonging to devices infected by the Glupteba

[17] See Exhibit 6, which is a true and correct copy of the webpage https://push.farm as of November 2, 2021, and Exhibit 7, which is a true and correct copy of the webpage https://trafspin.com as archived by the WayBack Machine on March 2, 2021.

[18] See Exhibit 8, which is a true and correct copy of the webpage https://www.awmproxy.net as of November 2, 2021. On November 23, 2021, AWMProxy.net was rebranded as Vd.net. A blog post on the same day claimed new ownership. *See The Project Has a New Domain and New Owners!*, Vd.net (Nov. 23, 2021), https://vd.net/news/the-project-has-a-new-domain-and-new-owners.html ("Dear friends! We are glad to inform you that our project has been sold to new owners. In this regard, we expect new positive changes and you can already see the first one of them - we have a new website address! We are sure that the new team

malware.[19] Cybercriminals and other customers pay the Glupteba Enterprise for the ability to use the infected devices' IP addresses to "proxy" or relay their internet activity to disguise their identity and location without any knowledge or consent by the users of the infected devices.

66. When a cybercriminal uses the location of an infected device as a proxy, the cybercriminal's requests (*e.g.*, his or her activity on the internet) will appear to be emanating from the location of the infected device, rather than the proxy user's true location. The use of proxies thereby enables cybercriminals to hide their tracks, avoid detection, and frustrate surveillance systems designed to detect and prevent activity from addresses believed to be associated with criminal and fraudulent activity.

67. Security systems that screen for suspicious IP addresses are less likely to detect a cybercriminal's activity if that criminal is using a proxy. The requests may not raise red flags or be detected by surveillance screens because they are relayed through the victims' devices. Similarly, the proxy activity helps mask cybercriminals' whereabouts and activity from law enforcement investigations.

68. AWMProxy.net claims on its website that it could provide over 10,000 proxies per month for $190, and over 200,000 per month for $690.[20] In addition, it touts that the proxies it sold have "frequent IP changes," and that it refreshed 3% of

will breathe new life into the project!"). *See* Exhibit 9, which is a true and correct copy of the webpage https://www.vd.net as of November 24, 2021.

[19] See Exhibit 10, which is a true and correct copy of the webpage https://abm.net as archived by the WayBack Machine on February 11, 2021.

[20] *See* Exhibit 8.

its proxies every 15 minutes.[21] An analysis of the IP addresses used by Dont.farm and AWMProxy.net indicate they use many common IP addresses, supporting the connection between the two schemes.

69. Abm.net's website offered a "wide selection of geopositions" and internet-service providers, permitting users to choose the country and city of the proxy they purchase.

70. Abm.net claimed that its proxy servers were compatible with Google, Gmail, YouTube, and other platforms.

71. In addition to being used to set up fraudulent Google accounts, proxies can be used to facilitate fraudulent or other improper online ad campaigns. That is, because the user of a proxy like AWMProxy.net can spread a large purchase of advertisements across multiple proxy IP addresses, the user can execute the advertising campaign while avoiding algorithms intended to detect improper ad campaigns and block the user's accounts. In other words, the proxies enable users to purchase ads as if the purchases came from many different (and valid) Google accounts, unbeknownst to the true holders of these Google accounts.

72. Proxy services such as AWMProxy.net and Abm.net attempt to hinder investigations by Google security teams such as TAG. IP addresses are a common factor used in identifying harmful activity, and by relaying efforts through residential proxies, bad actors are more likely to avoid detection and successfully undertake

[21] *Id.*

harmful activities such as launching malicious or fraudulent Google Ad campaigns and sending phishing emails to Google users.

73. Each year, Google spends millions of dollars protecting its Ads platform and in protecting Google users. Proxy services like AWMProxy.net and Abm.net, which blatantly and publicly advertise and instruct how to create fraudulent Google accounts, take up significant Google resources to counter.

Cryptojacking and Other Criminal Schemes

74. "Cryptojacking" involves secretly exploiting the computing and processing power of infected devices to generate, or "mine," cryptocurrency.

75. The Glupteba Enterprise uses the collective computing power of infected devices to "mine" cryptocurrency for the benefit of the Enterprise.

76. The Enterprise's hijacking of infected devices for this purpose results in harm to the owners of the infected devices, who are generally unaware that their device has been co-opted for this purpose. This harm includes the impairment of the device's computing and processing power to perform tasks at the direction of the true owner, and also the cost of the electricity that is consumed by the mining activity.

77. In addition, because the Enterprise is capable of deploying any type of malware to infected devices, the power of the Glupteba botnet may be harnessed, at any time, to conduct other cybercrimes. For example, it could be used to execute a powerful DDoS attack, which would flood a legitimate business's website with requests for the purpose of rendering it inoperable. Or, it could be used to conduct ransomware attacks on legitimate businesses of all sizes. In a ransomware attack,

the ransomware encrypts the computer system's files, rendering these files and the systems that rely on them unusable, and the victim is extorted to pay money in order for the malicious actors who deployed the ransomware to decrypt the files and restore access.

VI. The Enterprise's Use of Corporate Entities

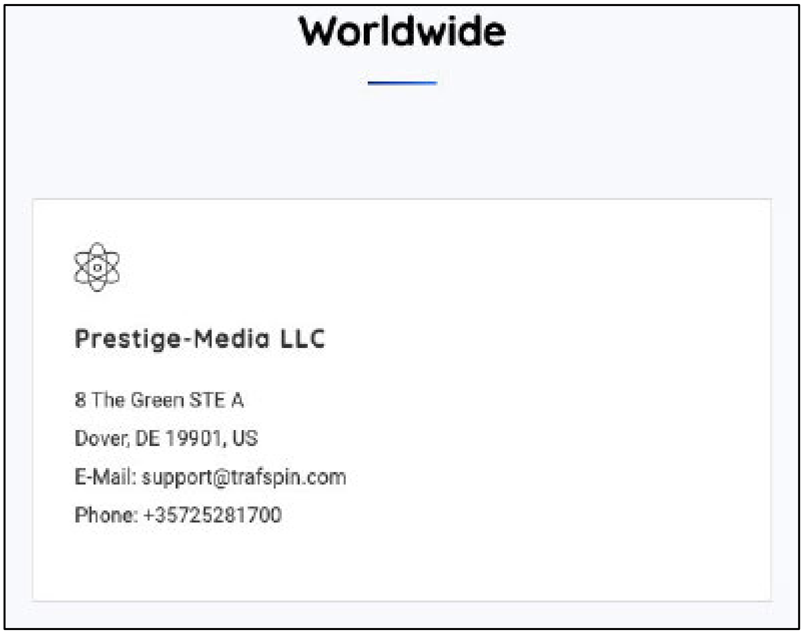
78. Through our investigation of the criminal activity of the Enterprise, we found that the Enterprise supported itself with several corporate entities:

79. **Prestige-Media LLC** ("Prestige-Media") is a Delaware limited-liability company used to support Trafspin.com's and Push.farm's operations. Prestige-Media is listed as the U.S. entity on Trafspin.com, as shown below.[22] The address provided for Prestige-Media is 8 The Green, Suite A, Dover, Delaware 19901, which is the same address as its registered agent, A Registered Agent, Inc.[23] That address is also used by Abm.net, and AWMProxy.net. Prestige-Media owns QIP.ru, which claims to be behind the website Extracard.net.[24]

[22] See Exhibit 11, which is a true and correct copy of the webpage https://trafspin.com/contacts as archived by the WayBack Machine on December 5, 2020.

[23] See Exhibit 12, which is a true and correct copy of the certificate of incorporation for Prestige-Media LLC.

[24] See Exhibit 13, which is a true and correct copy of a certified translation of the webpage https://career.habr.com/companies/qip as of November 14, 2021.



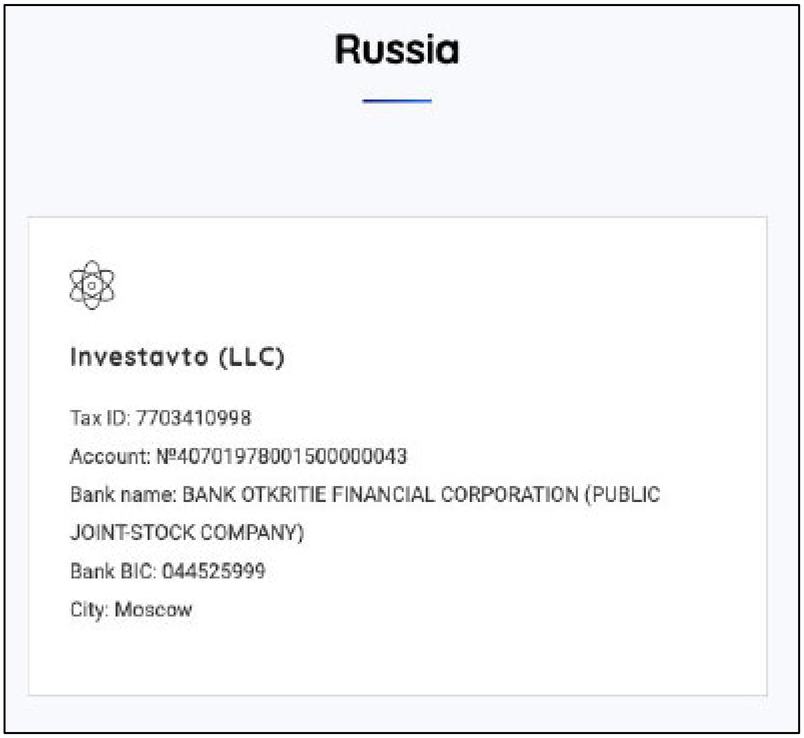
Worldwide

Prestige-Media LLC

8 The Green STE A
Dover, DE 19901, US
E-Mail: support@trafspin.com
Phone: +35725281700

80. **Investavto LLC** is a Russian limited-liability company based in Moscow that supports Trafspin.com's and Push.farm's operations in Russia and appears to be supported by Prestige-Media LLC in the United States. Investavto was registered on May 26, 2016, and its legal address is 123112, Moscow, Presnenskaya Embankment 12, Office 5.[25] Investavto LLC is listed as the Russian corporate entity on the website Trafspin.com. Below is a true and correct excerpt from the Trafspin.com website.[26]

[25] See Exhibit 14, which is a true and correct copy of a certified translation of an extract for Investavto LLC's from Russia's Uniform State Register of Legal Entities as of November 3, 2021.
[26] *See* Exhibit 11.



Russia

Investavto (LLC)

Tax ID: 7703410998

Account: №40701978001500000043

Bank name: BANK OTKRITIE FINANCIAL CORPORATION (PUBLIC JOINT-STOCK COMPANY)

Bank BIC: 044525999

City: Moscow

81. **Valtron LLC** is a Russian limited-liability company based in Moscow that appears to be used to support the Glupteba Enterprise. Valtron LLC was incorporated on August 23, 2019. Its legal address is listed as Presnenskaya Embankment 12 (Federation Tower),[27] which is also associated with Investavto LLC and Trafspin.com. Recent Valtron job postings state that Valtron's website is

[27] See Exhibit 15, which is a true and correct copy of a certified translation of an extract for Valtron LLC's from Russia's Uniform State Register of Legal Entities as of November 3, 2021.

"Trafspin.com".[28] Notably, the job postings include requirements that the candidates have experience with Google and other technology-company advertising.[29]

82. An archived website indicates that Valtron LLC operated a website called "**Voltronwork.com**."[30] For example, a "copyright" stamp at the bottom of Voltronwork.com was attributed to Valtron LLC.[31] And Valtron was listed as the contact for Voltronwork.com on its website.[32]

83. Voltronwork.com, which now appears to be operating as "Undefined.team,"[33] recruits developers to support the Enterprise's websites, transactions, and overall operation. While Voltronwork.com's website is not currently live, an internet archive version indicates it marketed itself as a advertising and software development company.[34]

[28] See, for example, Exhibit 16, which is a true and correct copy of a certified translation of a job posting for an Affiliate Manager, accessed on November 14, 2021, on employmentcenter.ru. The posting states that the applicant must be experienced with Google AdWords and Google Analytics.

[29] See, for example, Exhibit 17, which is a true and correct copy of a certified translation of a job posting for an iOS Developer, accessed on November 14, 2021, on employment-services.ru. The posting states that the applicant must be experienced with developing simple mobile applications for advertising with Google and other technology companies.

[30] See Exhibit 18, which is a true and correct copy of a certified translation of the webpage https://voltronwork.com as archived by the WayBack Machine on July 26, 2021.

[31] *See id.*

[32] *See id.*

[33] See Exhibit 19, which is a true and correct copy of a certified translation of the webpage https://undefined.team as archived by the WayBack Machine on June 17, 2021.

[34] *Id.*

84. Voltronwork.com used Google advertisements to post job openings for the websites effectuating the above criminal schemes.[35] Specifically, job advertisements for Voltronwork.com linked to Trafspin.com, and the registered companies behind Trafspin.com were Prestige-Media and Investavto, which, as explained *infra* at paragraphs 78 to 80, support various criminal schemes.[36] Additionally, a September 2021 job posting by Undefined.team for an HTML Coder stated that Extracard.net and Abm.net were projects of the "large IT team UNDEFINED.TEAM."[37] And multiple reviews of Voltronwork.com found on Russian-language employment review sites tie together Voltronwork.com, Dont.farm, and how the businesses are involved in stealing user accounts.[38]

85. Voltronwork.com is responsible for the development of AWMProxy.net, Abm.net, Dont.farm, Trafspin.com (Push.farm), and Extracard.net. Examination of Glupteba code revealed that the URL of a subdomain of Voltronwork.com, git.voltronwork.com, was inadvertently left visible in the malware's code, of a September 2020 variant of the Glupteba malware proxy module. It is believed this was inadvertent as it directly references the Enterprise's entity, rather than pointing

[35] See, for example, Exhibit 20, which is a true and correct copy of a certified translation of a screenshot of a job posting for a Technical Director, posted on November 2, 2019. The posting lists the website as Trafspin.com and the human resources contact email as "nana@voltronwork.com."

[36] *Id.*

[37] See, for example, Exhibit 21, which is a true and correct copy of a certified translation of a job posting for a HTML Coder, accessed on November 3, 2021, on moskva.jobfilter.ru.

[38] See, for example, Exhibits 22 and 23, which are true and correct copies of certified translations of reviews of Voltronwork.com on the websites ne.orabote.net, and detected-job.ru, respectively.

to an anonymous domain that acted as a proxy, which was a technique they utilized throughout their code. Moreover, in 2020, git.voltronwork.com shared the same server (5.188.184.37) as Gitlamp.com, which has been observed in other Glupteba binary files.[39] Additionally, an IP address once connected to vpn.voltronwork.com, was the Terms of Service IP for Google email accounts that contained within their addresses the words "voltron", "voltronwork", "valtron", "awm-proxy" and "card.farm." That same IP address also was used to log into Google accounts from domains associated with Dont.farm, AWMProxy.net, Voltronwork.com, and Undefined.team. Furthermore, a job listing for a technical director position with Valtron, shows the recruiter contact information with an email on the @voltronwork.com domain, listing their website as Trafspin.com and as having a physical address at the Federation Tower in Moscow, which is the same address used by Investavto and Valtron.

VII. Glupteba Enterprise: Individuals

86. We identified two individuals who control or participate in the Glupteba Enterprise's criminal schemes:

87. **Dmitry Starovikov** is directly tied to a former Glupteba botnet C2 server. Based on its investigation, Google determined that a server with the IP address 82.204.203.174 was a C2 server used by the Glupteba Enterprise specifically for directing the deployment of proxies onto infected machines. Google's investigation

[39] 5.188.184.37, VirusTotal (accessed November 30, 2021), https://www.virustotal.com/gui/ip-address/5.188.184.37/relations.

also revealed that when Dmitry Starovikov signed up for a Google account and executed Google's "Terms of Service," he did so from the same IP address, 82.204.203.174.

88. In addition, Dmitry Starovikov has an email account under the Voltronwork.com domain, and acts as an administrator for the Voltronwork.com Google Workspace account. Additionally, the secondary email address for the Workspace Voltronwork.com account, is an email containing Dmitry's name under the Trafspin.com domain. Dmitry Starovikov resides in Russia.

89. **Alexander Filippov** is directly tied to a former Glupteba botnet C2 Server in the same manner as Dmitry Starovikov. In addition, Filippov has email accounts associated with the Google Workspace accounts related to Voltronwork.com, Dont.farm, and Undefined.team. Moreover, Filippov's Undefined.team account has a recovery email address that has a billing name of Alexander Filippov and lists the Federation Tower as the billing address, which is used by many other connected entities in the Enterprise, as discussed above.

VIII. The Botnet Has Inflicted Serious Harm On Internet Users

90. TAG estimates that the Glupteba botnet comprises 1 million or more infected devices. Each of these devices is vulnerable to illegal access, use and theft of sensitive information, including financial account information, and even the contents of personal emails.

91. This past year, TAG has been collaborating with security teams across Google to disrupt Glupteba malware activity involving Google services. Google has

terminated approximately 63 million Google Docs, 1,183 Google Accounts, 909 Cloud Projects, and 870 Google Ads accounts associated with the distribution or use of Glupteba malware. Google provided approximately 3.5 million Google Safe Browsing warnings, thereby helping to protect approximately 2 million users from interacting with known Glupteba malware domains hosted on the web.

92. Google analyzed a sample of logs from its public DNS resolver to assess the impact of the Glupteba botnet on Google users in New York City. Extrapolating from that sample, Google conservatively estimates that thousands of infected devices in New York City have connected to Glupteba domains through the Google DNS (and many more may have connected through DNS operated by entities other than Google).

93. The Glupteba Enterprise also threatens Google and the safety and security of Google's products, including Gmail, YouTube, and AdWords. The Enterprise has, for example, fraudulently purchased ad sales from Google in connection with the Credit Card Fraud scheme.

94. The Glupteba Enterprise threatens both the actual security of Google's systems and Google's reputation for security. The Glupteba botnet is used both to steal Gmail credentials and to send emails from the user's account to further spread malware. The botnet also steals data from Google's Chrome internet browsers. And as discussed above, users download the Glupteba malware through a fake website deceiving users into believing they are downloading a video from Google's YouTube

video sharing platform. These actions cause harm to Google users, and impair Google users' confidence and trust in Google, its services, and its platforms.

95. TAG personnel have spent more than 2,000 hours investigating the Glupteba botnet and seeking to protect Google and its users from its misconduct. These efforts by TAG have cost Google substantial amounts of money, far in excess of $100,000. The personnel of several other Google teams also have been involved in investigating and deterring the Glupteba malware, further increasing the harm and expense incurred by Google.

96. Beyond Google and Google users, the continued proliferation of malware on Google platforms is a threat to the internet ecosystem as a whole. Court intervention requested herein is a necessary step to deter the prevention of further abuses.

IX. Disrupting the Glupteba Botnet

97. Due to the Glupteba botnet's sophisticated architecture and the actions that its organizers have taken to maintain the botnet (including the use of blockchain technology to prevent disruption), I believe that if the operators of the botnet were provided advance notice that the domains and IP addresses being used by the botnet would be disabled, the operators would take measures to ensure the botnet's survival and frustrate any disruption efforts.

98. Based on my experience in investigating and disrupting similar threats, I believe that the most effective way to suspend the injury caused by the Glupteba botnet is to:

a. Direct the relevant hosting companies to disable the IP addresses of the Enterprise's servers;

b. Direct the relevant DNS providers to suspend all known domain names and prevent them from being transferred or changed;

c. Direct the relevant domain registrars to suspend all known domain names and prevent them from being transferred, changed, or resold;

d. Render inaccessible any content stored on its C2 servers;

e. Direct the hosting companies and registrars to suspend all services to the botnet operators, not to warn or aid the operators, and not to enable the circumvention of the order;

f. Block any efforts by the operators to purchase or lease additional servers;

g. Direct the Defendants to suspend transactions to the known Bitcoin blockchains that act as a failsafe for the Glupteba botnet;

99. I believe that the only way to effectively disrupt the botnet and to address the harm caused to Google, its users, and the public, is to take the steps described in the Proposed Ex Parte Temporary Restraining Order and Order to Show Cause For a Preliminary Injunction. This relief will imperil the botnet's monetization and operational control and interrupt its harmful activities.

100. It is crucial that the disruption steps outlined above and in the proposed temporary restraining order be carefully coordinated. In particular, that the malicious domains and IP addresses are directed by the Court to be turned off

immediately upon receipt of any order. Any delay could warn the operators of this action and result in immediate relocation of the C2 servers or other botnet infrastructure. In addition, because the Glupteba botnet's C2 structure is diffuse and globally distributed, Google is coordinating relief with other private parties, authorities, and in other jurisdictions. The proposed temporary restraining order is designed to enable coordinated efforts that will maximize the impact of the disruption efforts.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on November 29, 2021, in Sunnyvale, California.

Shane Huntley